

Axway Secure Messenger

Protegete la vostra azienda con la crittografia delle email basata su policy



Tutte le organizzazioni vogliono evitare di passare alle cronache per una fuga di dati, specialmente per una fuga accidentale di informazioni sensibili causata da un dipendente che ha erroneamente inviato un'email o un allegato non sicuro all'indirizzo sbagliato. Le conseguenze di questo tipo di violazione della sicurezza possono essere devastanti e includono ad esempio la perdita di dati, l'interruzione del business, danni al marchio e alla reputazione, nonché dispute e sanzioni normative.

Axway Secure Messenger™ è in grado di mettere la vostra azienda al riparo da queste minacce migliorando la sicurezza delle email, la governance e la conformità. Combinando un relay SMTP all'avanguardia con potenti funzionalità di filtro dei contenuti basate su policy, Secure Messenger ispeziona tutte le email in entrata e in uscita presso il gateway Internet per identificare i contenuti dei messaggi o dei file allegati che violano le policy di sicurezza definite dall'azienda e reindirizza automaticamente i messaggi sospetti verso un canale sicuro affinché vengano recapitati in modalità crittografata, messi in quarantena, eliminati o sottoposti ad altre operazioni. Questo approccio perimetrale garantisce che tutti gli utenti, sia quelli interni sia quelli esterni, rispettino sempre le policy aziendali, senza dover implementare o gestire attivamente un software di crittografia sui desktop o modificare gli schemi di utilizzo comune.

Caratteristiche principali e vantaggi

Funzionalità di crittografia complete

Comunicazioni email inbound e outbound sicure, indipendentemente dal canale: gateway-to-gateway, gateway-to-desktop o recapito di messaggi basato sul Web

- Crittografia e autenticazione dei messaggi in base a policy centralizzate e instradamento automatizzato dei messaggi
- Utilizzo delle email per divulgare informazioni e asset aziendali riservati e per documentare transazioni aziendali sensibili
- Distribuzione di funzionalità email sicure a qualsiasi dipendente, cliente o partner, senza necessità di installare o apprendere l'utilizzo di un nuovo software. Crittografia automatica gateway-to-gateway che non richiede alcun intervento da parte dell'utente finale

Potente gestione delle policy email

Impostazione e gestione delle policy per analizzare, gestire, proteggere, tracciare e segnalare il flusso del traffico email all'interno o all'esterno dell'organizzazione

- Prevenzione di fughe di dati accidentali resa possibile dal semplice filtraggio dei contenuti della casella di posta, da un intuitivo sistema di gestione delle policy e dalla crittografia automatica gateway-to-gateway
- Sfruttamento delle applicazioni e delle reti esistenti con la registrazione di una password e servizi di gestione facile integrazione con i sistemi di gestione di identità di terze parti
- Definizione e applicazione delle policy di messaggistica a livello di dominio, gruppo o individuale



Caratteristiche principali e vantaggi**Governance e conformità normativa semplificate**

Semplificazione della conformità con standard di settore e norme governative in continua evoluzione grazie a dizionari specializzati e funzionalità di scansione e monitoraggio migliorate

- Creazione di filtri di contenuti per identificare le informazioni personali protette da leggi quali il PCI Data Security Standard statunitense, la Direttiva sulla protezione dei dati dell'UE e la legge sulla protezione dei dati personali giapponese
- Scansione di messaggi e allegati eseguita da un dizionario di servizi finanziari allo scopo di individuare informazioni finanziarie aziendali e personali e semplificarne la conformità con SOX, GLBA e altre normative
- Scansione eseguita da un dizionario HIPAA allo scopo di individuare informazioni sanitarie protette (PHI) per attuare la conformità con HITECH/HIPAA e altre normative sanitarie
- "Traccia cartacea" documentata creata a scopo di audit e conformità tramite il monitoraggio del recapito dei messaggi al desktop del destinatario

La soluzione di crittografia dei dati delle email più accessibile

Dal momento che in genere un'azienda non può imporre software desktop speciali per l'invio o la ricezione di email sicure al di fuori della rete aziendale, Secure Messenger offre un'ampia serie di metodi di recapito dei messaggi basati solo su client email e browser Web standard; in altri termini, non è necessario installare né gestire alcun software desktop.

Recapito pull online tramite un browser Web (Secure Webmail)

Secure Webmail utilizza un link Web incorporato in un messaggio email per reinstradare il destinatario a un server sicuro affinché legga il messaggio su un browser Web. Questa metodologia sfrutta le funzionalità di crittografia SSL esistenti del browser per il recapito di messaggi sicuri e supporta al contempo metodi di autenticazione basati su browser per garantire che solo il destinatario corretto visualizzi il messaggio.

I destinatari possono accedere ai messaggi ovunque su Internet, nonché rispondere utilizzando lo stesso canale sicuro. Tutti gli utenti dispongono di una casella di posta basata sul Web sicura (Secure Inbox) che consente loro di inviare, ricevere, ordinare, eliminare, salvare e organizzare i messaggi ovunque su Internet.

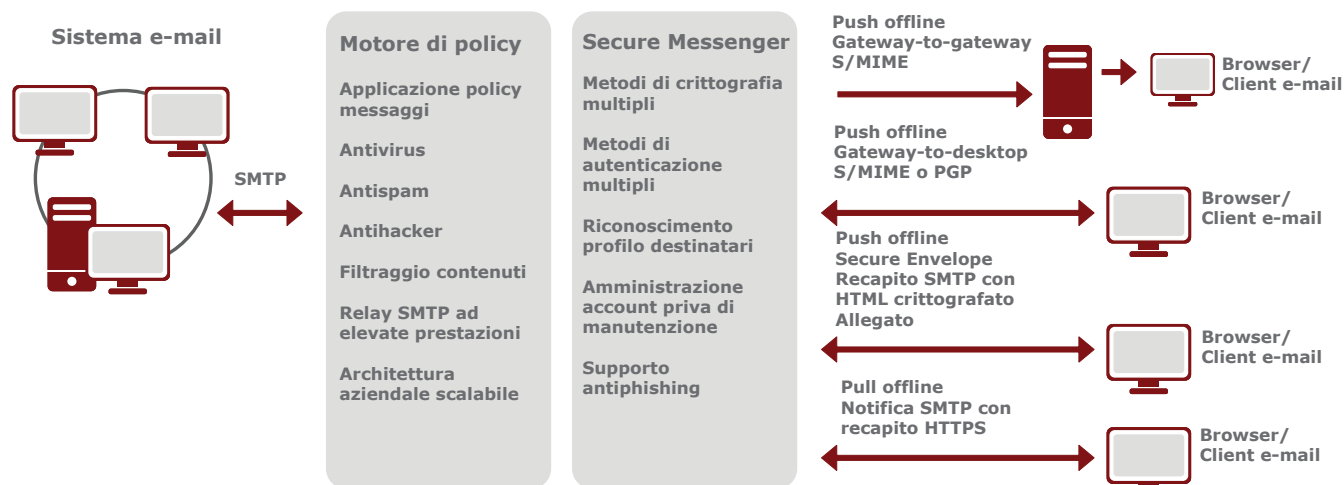
Recapito push offline tramite un browser Web (Secure Envelope)

Secure Envelope recapita un messaggio crittografato direttamente nella casella di posta di un destinatario utilizzando un'email SMTP standard come mezzo di trasporto, ma include il contenuto del messaggio crittografato in un allegato HTML. I destinatari aprono l'allegato tramite un browser online o offline e immettono una password per decrittografare e leggere il messaggio.

Recapito push offline tramite S/MIME

Se il certificato digitale di un destinatario è disponibile per la crittografia e l'infrastruttura email del destinatario supporta lo standard S/MIME, Secure Messenger supporta il recapito push offline sia tramite la crittografia S/MIME gateway-to-gateway che gateway-to-desktop.





Sicurezza delle email all-inclusive

- La distribuzione di Axway Secure Messenger su un'appliance Linux protetta con hardening con supporto di IPv6 insieme ad Axway MailGate, una soluzione per la sicurezza delle email in ingresso e in uscita di livello enterprise, permette di risolvere tutti i problemi di sicurezza delle email con una soluzione completa su un'unica appliance.
- Le licenze di Secure Messenger e MailGate sono disponibili insieme o separate. È possibile attivare entrambe le soluzioni contemporaneamente o nel tempo, al variare delle esigenze aziendali.
- Un'unica installazione guidata, un'unica interfaccia di amministrazione e un'unica interfaccia per gli utenti finali aumentano la semplicità di installazione e utilizzo.

Opzioni di consegna

- Appliance Linux protetta tramite hardening
- Appliance Axway/Dell
 - Appliance Virtual VMware

Elevata disponibilità/Disaster Recovery

- Le funzionalità di disaster recovery consentono di conservare intatta la posta elettronica a seguito di perdite di dati catastrofiche o guasti irreparabili del server con il ripristino dei dati sottoposti a backup.
- Utilizzando un NAS (Network-Attached Storage) è possibile abilitare un'effettiva alta disponibilità basata sulle applicazioni, per una funzionalità ininterrotta in caso di guasti o errori di sistema.

Ulteriori informazioni

Per ulteriori informazioni su come Axway Secure Messenger può proteggere la vostra azienda dalla minaccia di fughe di dati data migliorando la sicurezza delle email, la governance e la conformità, inviare un'email all'indirizzo axwaysolutions@axway.com o visitare il sito www.axway.it/contattaci.

Per Ulteriori informazioni, visit www.axway.it

Copyright © Axway 2011. Tutti i diritti riservati.

